

(19)日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表2002-542672

(P2002-542672A)

(43)公表日 平成14年12月10日(2002.12.10)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	特記事項(参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
G 0 6 F 12/14	3 2 0	15/00	3 3 0 A 5 B 0 3 5
15/00	3 3 0	G 0 9 C 1/00	6 6 0 G 5 B 0 8 5
G 0 6 K 19/00		H 0 4 L 9/00	6 0 1 B 5 J 1 0 4
19/07		G 0 6 K 19/00	N

審査請求 未請求 予備審査請求 有 (全 26 頁) 最終頁に続く

(21)出願番号 特願2000-611462(P2000-611462)  
 (86)(22)出願日 平成12年3月31日(2000.3.31)  
 (85)翻訳文提出日 平成13年10月10日(2001.10.10)  
 (86)国際出願番号 PCT/EP00/02918  
 (87)国際公開番号 WO00/62505  
 (87)国際公開日 平成12年10月19日(2000.10.19)  
 (31)優先権主張番号 99/04767  
 (32)優先日 平成11年4月13日(1999.4.13)  
 (33)優先権主張国 フランス(FR)

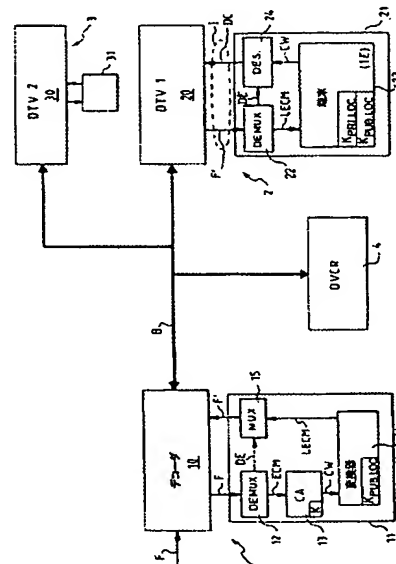
(71)出願人 トムソン ライセンシング ソシエテ ア  
 ノニム  
 Thomson Licensing  
 S. A.  
 フランス国, エフ-92100 ブローニュ  
 ビヤンクール, ケ アルフォンス ル  
 ガロ, 46番地  
 (72)発明者 ケ, フロランス  
 フランス国, 13006 マルセイユ, リュ・  
 ド・ブルトウイユ 169, レ・オー・ド・  
 ブルトウイユ アパルトマン62 パティマ  
 アン  
 (74)代理人 弁理士 伊東 忠彦

最終頁に続く

(54)【発明の名称】 デジタルホームネットワークとデジタルホームネットワークの作成及び更新方法

## (57)【要約】

ローカルデジタルネットワークは、ネットワークの外部から発するデータを受信し、そのデータをネットワークのあるポイントへ送信するアクセス装置(1)と、ネットワーク内を流れるデータを受信し、そのデータをネットワークのあるポイントで提示する提示装置(2, 3)と、を有する。データは、ネットワーク内を暗号形式で流れ、ネットワークの全ての装置は、ネットワークにおけるデータの暗号化及び復号化用のローカル鍵である単一の鍵を使用する。好ましくは、ネットワークのローカル鍵は、公開鍵と秘密鍵のペアにより形成される。このネットワークの目的は、このローカルネットワーク内でのデータのコピーを許可し、他のネットワークを宛先とする不正コピーを禁止することである。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項1】 ネットワークの外部から発するデータを受信し、該ネットワークのあるポイントへ送信することができる少なくとも一台のアクセス装置（1）と、

ネットワークのあるポイントで提示すべく、ネットワークを流れるデータを受信するよう適応した少なくとも一台の提示装置（2，3）と、  
を有し、

データは暗号形式だけで流れるように適応している、ローカルデジタルネットワーク、特に、デジタルホームネットワークであって、

該ネットワークの全ての装置は、ネットワークを流れるデータの暗号化及び復号化のため、ネットワークに特有の単一の暗号鍵であるネットワークのローカル鍵（ $K_{PUB. LOC}$ ， $K_{PRI. LOC}$ ）を使用することを特徴とする、デジタルネットワーク。

【請求項2】 データは公開鍵暗号システムを用いて暗号化され、

ネットワークの該ローカル鍵は、公開鍵と秘密鍵のペアであるローカル公開鍵（ $K_{PUB. LOC}$ ）及びローカル秘密鍵（ $K_{PRI. LOC}$ ）により構成されることを特徴とする、請求項1記載のデジタルネットワーク。

【請求項3】 該ネットワークに接続された提示装置（2，3）だけがローカル秘密鍵（ $K_{PRI. LOC}$ ）を保持することを特徴とする請求項2記載のデジタルネットワーク。

【請求項4】 所与の時点で、ネットワークの単一の提示装置は、ローカル秘密鍵（ $K_{PRI. LOC}$ ）を、該ネットワークへ接続するよう適した新しい提示装置へ送信するよう許可されていることを特徴とする請求項3記載のデジタルネットワーク。

【請求項5】 所与の時点で、提示装置は、

i）提示装置が最初にネットワークへ接続されたときのバージン状態（ $IE = 00$ ）である第1の状態と、

ii）提示装置が、ネットワークのローカル秘密鍵を、ネットワークへ接続するのに適した新しい提示装置へ送信することが許可された親状態（ $IE = 01$ ）

である第2の状態と、

i i i) 提示装置は、ネットワークのローカル秘密鍵を、ネットワークへ接続する適性を備えた新しい提示装置へ送信することが許可されなくなる無効状態 ( I E = 1 0 ) である第3の状態と、

の三つの状態の中でただ一つの状態だけを取ることができ、

提示装置は、上位ランクの状態へ移る場合に限り状態を変更するよう適応している、

ことを特徴とする請求項3記載のデジタルネットワーク。

【請求項6】 ネットワークの単一の提示装置が、第2の状態、すなわち、ネットワークの親である親状態にあることを特徴とする請求項5記載のデジタルネットワーク。

【請求項7】 所与の時点で、ネットワークの親は、該ネットワークに最後に接続された提示装置であることを特徴とする請求項6記載のデジタルネットワーク。

【請求項8】 請求項2乃至7のうちいずれか一項記載のデジタルネットワークに接続するよう適応した提示装置であって、

所与の時点で、該提示装置は、

i) 提示装置が最初にネットワークへ接続されたときのバージン状態 ( I E = 0 0 ) である第1の状態と、

i i) 提示装置が、ネットワークのローカル秘密鍵を、ネットワークへ接続するのに適した新しい提示装置へ送信することが許可された親状態 ( I E = 0 1 ) である第2の状態と、

i i i) 提示装置は、ネットワークのローカル秘密鍵を、ネットワークへ接続する適性を備えた新しい提示装置へ送信することが許可されなくなる無効状態 ( I E = 1 0 ) である第3の状態と、

の三つの状態の中でただ一つの状態だけを取ることができ、

提示装置は、上位ランクの状態へ移る場合に限り状態を変更するよう適応している、

ことを特徴とする提示装置。

【請求項9】 該提示装置がバージン状態にあるとき、該提示装置は、固有の公開鍵と秘密鍵のペアを保持し、接続されるのに適したネットワークのローカル鍵のペアを受信することが許可され、固有の鍵のペアの代わりに受信したローカル鍵のペアを保持することを特徴とする、請求項8記載の提示装置。

【請求項10】 該提示装置が無効状態にあるとき、該提示装置は、接続されるネットワークのローカル鍵のペアを受信することが許可されなくなる、請求項8又は9記載の提示装置。

【請求項11】 該提示装置は、該提示装置が占める状態を保持する記憶手段を有し、この記憶手段はスマートカードに統合されている、ことを特徴とする請求項8乃至10のうちいずれか一項記載の提示装置。

【請求項12】 ネットワークのローカル鍵のペアは、上記提示装置に装備されたスマートカード内に収容されていることを特徴とする、請求項8乃至11のうちいずれか一項記載の提示装置。

【請求項13】 請求項5乃至7のうちいずれか一項記載のローカルデジタルネットワークを作成する方法であって、

デジタルバス(B)を介して、アクセス装置(1)と、公開鍵( $K_{PUB2}$ )及び秘密鍵( $K_{PR12}$ )のペアを収容するバージン状態の提示装置(2)とを接続するステップ(a)と、

提示装置(2)において、該バス(B)を介して公開鍵( $K_{PUB2}$ )を配布するステップ(b)と、

アクセス装置(1)において、該公開鍵( $K_{PUB2}$ )を受信し、公開鍵をネットワークの新しいローカル鍵( $K_{PUB,LOC} = K_{PUB2}$ )として保持し、該バスを介して、提示装置の状態変更信号を配布するステップ(c)と、

提示装置(2)において、該状態変更信号を受信し、親状態( $IE = 01$ )へ移るステップ(d)と、  
を有することを特徴とする方法。

【請求項14】 バージン状態( $IE = 00$ )にあり、公開鍵( $K_{PUB3}$ )及び秘密鍵( $K_{PR13}$ )を保持する新しい提示装置(3)を、請求項5乃至7のうちいずれか一項記載のローカルデジタルネットワークへ接続する方法であ

って、

新しい提示装置 ( 3 ) をデジタルバス ( B ) を用いて該ローカルネットワークへ接続するステップ ( e ) と、

新しい提示装置 ( 3 ) において、該バス ( B ) を介して、公開鍵 (  $K_{PUB3}$  ) を配布するステップ ( f ) と、

該ネットワークの少なくとも一台のアクセス装置 ( 1 ) において、新しい提示装置の公開鍵 (  $K_{PUB3}$  ) を受信し、該アクセス装置が既にネットワークの公開鍵であるローカル公開鍵 (  $K_{PUB.Loc}$  ) を保持しているかどうかを照合し、保持している場合に、該バス ( B ) を介して、ネットワークのローカル公開鍵を配布するステップ ( g ) と、

新しい提示装置 ( 3 ) において、ネットワークのローカル公開鍵 (  $K_{PUB.Loc}$  ) を受信し、ローカル公開鍵を記憶し、該バスを介して、ネットワークの全ての提示装置を宛先として、親状態の提示装置からの応答を要求する応答要求信号を配布するステップ ( h ) と、

ネットワークの親提示装置 ( 2 ) において、応答要求信号を受信し、無効状態 (  $IE = 10$  ) へ移り、新しい提示装置 ( 3 ) に応答して、ネットワークローカル秘密鍵 (  $K_{PR.Loc}$  ) を、新しい提示装置 ( 3 ) が復号化可能な暗号形式で配布するステップ ( i ) と、

新しい提示装置 ( 3 ) において、ネットワークの該ローカル秘密鍵 (  $K_{PR.Loc}$  ) を受信し、該ローカル秘密鍵を記憶し、受信承認信号を、ネットワークの前の親提示装置である提示装置 ( 2 ) へ配布するステップ ( j ) と、

ネットワークの前の親提示装置である提示装置 ( 2 ) において、該受信承認信号を受信し、状態変更信号を新しい提示装置 ( 3 ) へ配布するステップ ( k ) と、

新しい提示装置 ( 3 ) において、該状態変更信号を受信し、親状態 (  $IE = 01$  ) へ移るステップ ( l ) と、

を有する、方法。

## 【発明の詳細な説明】

## 【0001】

本発明は、一般的に、ローカルデジタルネットワークの分野に係り、特に、デジタルホームネットワークの分野に関する。

## 【0002】

このようなネットワークは、たとえば、IEEE 1394標準に準拠したバスのようなデジタルバスによって相互連結された装置の組により構成される。ネットワークは、2種類の装置、すなわち、

ローカルネットワークの外部から発したデータを受信し、ネットワークの接続されたあるポイントへそのデータを送信することができるアクセス装置と、

ネットワーク内を流れるデータをネットワークの接続された別のポイントへ提示するため、ネットワーク内を流れるデータを受信するよう適合した提示装置と

を有する。第2のタイプの装置は、ローカルネットワークの外部とのリンクを具備していない。

## 【0003】

オーディオ及び／又はビデオデータを住宅の種々の部屋へ伝達することを目的としたデジタルホームネットワークの一例を考えると、アクセス装置は、ネットワークの外部から、衛星アンテナ若しくはケーブルコネクションを介して、ビデオ番組を受信するデジタルデコーダ又はセットトップ・ボックス、或いは、光ディスクから読み出したデータ（オーディオ及び／又はビデオ）をデジタル形式でネットワーク上にブロードキャストする光ディスクの読取装置である（本例の場合に、ディスクはネットワークの外部から発したデータを収容する。）。提示装置は、たとえば、ネットワークから受信したビデオ番組を見ることができるテレビジョン受像機、或いは、より一般的には、受信したデジタル情報をエンドユーザへブロードキャストするため、受信したデジタル信号をアナログ形式に変換することができる装置である。

## 【0004】

上述のタイプのホームネットワークは、ネットワークの外部とのリンクを具備

せず、ネットワーク内を流れるデータを記録する機能を有する第3のタイプの装置を含む。この第3のタイプの装置の一例として、特に、デジタルビデオレコーダ、又は、DVD（デジタル汎用ディスク）タイプの光ディスクを記録することができる装置を挙げることができる。

【 0 0 0 5 】

全く同じ装置が、上述の二つ以上の異なる装置カテゴリーに属し得ることに注意する必要がある。たとえば、光ディスクを記録する装置は、商業的に予め記録されたディスクを読み取ることが可能であるため、上述の第1の装置のカテゴリーと第3の装置のカテゴリーに同時に属している。

【 0 0 0 6 】

ローカルネットワークの外部から発したデータを供給するコンテンツプロバイダ、特に、有料テレビ番組をブロードキャストするサービスプロバイダ、若しくは、たとえば、その他の光ディスクの発行元の立場を考えると、これらの伝送されたデータがコピーされること、及び、（たとえば、光ディスク若しくはその他の記録媒体へコピーされることによって）あるローカルネットワークから別のローカルネットワークへ容易に流出し得ることを防止する必要がある。

【 0 0 0 7 】

このため、実際には、鍵を使用する暗号化アルゴリズムを用いてデータを暗号化することにより、データを秘密形式で伝送することが知られている。この鍵は、これらのデータを受信することが許可されている装置に対し事前に公開されているか、或いは、コンテンツプロバイダとそれらの装置との間で特定の安全なプロトコルに従って交換される。

【 0 0 0 8 】

デジタルホームネットワークを保有するユーザの立場を考えると、これらのデータは、ネットワーク内の1台の装置がコンテンツプロバイダからデータを受信する権利を付与されているときには、ネットワークの他の全ての装置へ送信可能であることが望ましい。したがって、有料テレビサービスの加入者であり、かつ、（暗号形式で送信された）番組をラウンジに設置された（番組の復号化を許可された）セットトップ・ボックスで受信するユーザは、これらの番組を、たとえ

ば、寝室に設置されたテレビジョンで視聴できることを希望する。さらに、ユーザは、受信した番組を記録し、後で、たとえ、その有料テレビサービスの加入者ではなくなったときでも、ネットワークの数台の装置でその番組を視聴できることに関心がある。

【 0 0 0 9 】

コンテンツプロバイダの要望と、ユーザの要望とを考慮することにより、本発明は、ローカルデジタルネットワークで受信されたデータがネットワークの種々の装置の間で自由に流れ、そのデータがあるローカルネットワークから別のローカルネットワークへ流れることを阻止する手段の提供を目的とする。

【 0 0 1 0 】

この目的を達成するため、本発明が提案するローカルデジタルネットワーク、特に、デジタルホームネットワークは、

ネットワークの外部から発するデータを受信し、そのデータをネットワークのあるポイントへ送信することができる少なくとも一台のアクセス装置と、

データが暗号形式だけで流れるように適応したネットワーク内を流れるデータを受信するよう適応し、ネットワークのあるポイントでそのデータを提示する少なくとも一台の提示装置と、

を有する。本発明によれば、ネットワークの全ての装置は、ネットワークを流れるデータの暗号化及び復号化のため、ネットワークに特有の単一の暗号鍵、すなわち、ネットワークのローカル鍵を使用する。

【 0 0 1 1 】

各ローカルネットワークは、他のローカルネットワークのローカル鍵とは異なる固有のローカル鍵を保有するので、ローカルネットワークへ入った情報は、ネットワークの全ての装置が同じように読むことができるが、他のローカルネットワークで読むためにコピーすることはできない。より正確に表現すると、情報は、暗号形式でコピーすることができるが、その情報がコピーされたローカルネットワークとは異なる別のローカルネットワークにおいてその情報を再生できない。したがって、本発明は、コンテンツプロバイダの要望と、ユーザの要望の両方を満たす。



## 【 0 0 1 2 】

本発明の好ましい一局面によれば、データは、非対称暗号システムと呼ばれる、公開鍵による暗号システムを用いて暗号化される。ネットワークのローカル鍵は、本例の場合に、公開鍵と秘密鍵のペア、すなわち、ネットワークのローカル公開鍵とローカル秘密鍵とによって構成される。

## 【 0 0 1 3 】

好ましくは、ネットワークに接続された提示装置だけがローカル秘密鍵を知っている。

## 【 0 0 1 4 】

具体的な一実施例によれば、ある時点で、ネットワークの単一の提示装置は、ローカル秘密鍵を、ネットワークに接続するのに適した新しい提示装置へ送信することが許可される。この装置は、その後、ネットワークの「親」と呼ばれる。

## 【 0 0 1 5 】

ネットワークの「親」である装置が、特に、初期ローカルネットワークと同じローカル鍵を保有する不正ローカルネットワークを作成するため、ローカルネットワークから取り外されたとき、初期ローカルネットワークの装置は、ローカル秘密鍵を、初期ローカルネットワークに接続するため適した新しい提示装置へ送信し得なくなるので、初期ローカルネットワークは変更できなくなる。

## 【 0 0 1 6 】

本発明の他の局面によれば、所与の時点で、提示装置は、以下の状態の中でただ一つの状態だけを取ることができる。

## 【 0 0 1 7 】

i) 提示装置が最初にネットワークへ接続されたときのバージン状態である第1の状態。

## 【 0 0 1 8 】

i i) 提示装置が、ネットワークのローカル秘密鍵を、ネットワークへ接続するのに適した新しい提示装置へ送信することが許可された親状態である第2の状態。

## 【 0 0 1 9 】

i i i) 提示装置は、ネットワークのローカル秘密鍵を、ネットワークへ接続する適性を備えた新しい提示装置へ送信することが許可されなくなる無効状態である第3の状態。

【 0 0 2 0 】

提示装置は、上位ランクの状態へ移る場合に限り、すなわち、バージン状態から親状態へ、或いは、親状態から無効状態へ移る場合に限り、状態を変更することができる。

【 0 0 2 1 】

本発明の好ましい一局面によれば、ネットワークの単一の提示装置は、第2の状態、すなわち、ネットワークの親である親状態にある。

【 0 0 2 2 】

具体的な一実施例によれば、所与の時点で、ネットワークの親は、ネットワークに最後に接続された提示装置である。

【 0 0 2 3 】

したがって、ネットワークの親の称号は、ローカルネットワークに接続された新しい提示装置へ渡される。これにより、単一の親提示装置から始めて、同じローカル鍵を有するローカルネットワークを順番に作成する不正行為を可能にさせることが阻止される。

【 0 0 2 4 】

また、本発明は、上述のように、デジタルネットワークに接続されるよう適応し、所与の時点で、上述のバージン状態、親状態又は無効状態の中のいずれか一つの状態だけを取ることができ、上位ランクの状態へ移るような状態の変更だけを行うように適応した提示装置に関する。

【 0 0 2 5 】

本発明の一局面によれば、提示装置がバージン状態にあるとき、提示装置は、固有の公開鍵と秘密鍵のペアを保有し、接続されるのに適したネットワークのローカル鍵のペアを受信することが許可され、固有の鍵のペアの代わりに受信したローカル鍵のペアを保持する。

【 0 0 2 6 】

本発明の他の局面によれば、提示装置が無効状態にあるとき、提示装置は、接続される適性のあるネットワークのローカル鍵のペアを受信することが許可されなくなる。

【 0 0 2 7 】

本発明の他の局面によれば、提示装置は、上記提示装置が占める状態を保持する手段を有し、この記憶手段はスマートカードに統合されている。

【 0 0 2 8 】

本発明の更に別の局面によれば、ネットワークのローカル鍵のペアは、上記提示装置に装備されたスマートカード内に収容されている。

【 0 0 2 9 】

また、本発明は、上述のネットワークのようなネットワークを作成し、更新する方法に関する。この方法については後述する。

【 0 0 3 0 】

本発明のその他の特徴及び利点は、添付図面と共に、以下の本発明の具体的、例示的な実施例の説明から明らかになるであろう。

【 0 0 3 1 】

添付図面を通じて、本発明と、以下に説明する本発明の具体的な実施例とを理解するために重要な要素だけが示されている。

【 0 0 3 2 】

アクセス装置 1 と、2 台の提示装置 2 と、一般的に D V C R (デジタルビデオカセットレコーダの略) と称されるデジタルビデオレコーダ 4 とを含むデジタルホームネットワークが図 1 に示されている。装置 1、2、3 及び 4 の組立体は、たとえば、I E E E 1 3 9 4 標準に準拠した家庭用デジタルバス B に接続される。

【 0 0 3 3 】

アクセス装置 1 は、スマートカード 1 1 を装備したスマートカードリーダーを具備したデジタルレコーダ 1 0 を含む。このデジタルレコーダ 1 0 は、衛星アンテナ、又は、ケーブルネットワークに接続され、サービスプロバイダによって配信ビデオ番組を受信する。これらの番組は、たとえば、M P E G 2 フォーマットの

データのストリーム F で受信される。公知の方法で、これらの番組は、スクランブルをかけられた形式で伝送され、そのコンテンツは、制御語 C W によってスクランブルされている。これらの制御語は、それ自体が、伝送中に秘密の状態を保ったまま所与の暗号アルゴリズムに従って鍵 K を用いて暗号化された形式で、データストリーム F 中で伝送される。

【 0 0 3 4 】

かくして、サービスプロバイダによって許可されたユーザだけが（たとえば、申込料金の対価として）伝送されたデータを復号化する権能を付与される。このため、プロバイダは、許可されたユーザに、制御語 C W を復号化するため役立つ鍵 K を供給する。殆どの場合に、番組を受信する権能は、ユーザが自分の申込料金を支払う間に限られた一時的な権能である。したがって、鍵 K は、サービスプロバイダによって定期的に変更される。

【 0 0 3 5 】

本発明によれば、以下に説明するように、ユーザは、自分が加入している間に伝送された番組を記録し、自分が加入者ではなくなった場合でも、自分のネットワーク上で希望の頻度で番組を再生することができる。これに対し、データは、暗号形式で記録されるので、そのデータを記録したユーザのネットワーク以外のネットワークでそのデータを再生することができない。

【 0 0 3 6 】

図 1 において、ネットワークの状態は、全ての装置が図 2 及び 3 を参照して後述する処理に応じて接続されている状態である。

【 0 0 3 7 】

次に、デコーダ 10 によって受信されたストリーム F で伝送されたデータが処理される様子を説明する。当業者には公知のように、MPEG2 フォーマットに従って伝送されたデータの場合、データストリーム F は、一連のビデオデータパケット、オーディオデータパケット、及び、管理データパケットを含む。管理データパケットは、特に、制御メッセージ ECM（権利制御メッセージの略）を含む。制御メッセージ ECM では、ビデオパケット及びオーディオパケットで伝送されたデータにスクランブルをかけるため利用される制御語 C W が、鍵 K を用い

た暗号形式で伝送される。

【 0 0 3 8 】

このデータストリーム F は、スマートカード 11 へ送信され、スマートカード内で処理される。データストリーム F は、デマルチプレクサ回路 ( D E M U X ) 12 によって受信され、デマルチプレクサ回路は、E C M をアクセス制御回路 C A 13 へ送信し、スクランブルをかけられたビデオデータ及びオーディオデータの packets D E をマルチプレクシング回路 ( M U X ) 15 へ送信する。回路 C A は、鍵 K を保持し、E C M に收容された制御語 C W を復号化することが可能である。回路 C A は、これらの制御語 C W を変換器回路 14 へ送信する。本発明によれば、変換器回路 14 は、ネットワークのローカル公開鍵  $K_{P U B . L o c}$  を保持する。変換器回路 14 は、この鍵  $K_{P U B . L o c}$  を使用し、制御語 C W を暗号化し、ローカル公開鍵を使用して暗号化されたこれらの制御語を、制御メッセージ L E C M でマルチプレクシング回路 15 へ送信する。これらのメッセージ L E C M は、初期データストリーム F で受信されたメッセージ E C M と同じ機能を備えているが、メッセージ L E C M の場合に、制御語 C W は、サービスプロバイダの鍵 K を用いて暗号化されるのではなく、ローカル公開鍵  $K_{P U B . L o c}$  を用いて暗号化されている点が相違する。

【 0 0 3 9 】

マルチプレクシング回路 15 は、データ packets D E と、変換された制御メッセージ L E C M を、データストリーム F' として送信し、データストリーム F' はデコーダ 10 によって受信される。家庭用バス B のあちらこちらを流れるデータストリームは、このデータストリーム F' であり、データストリーム F' は、いずれか 1 台の提示装置 2 又は 3 によって受信され、或いは、デジタルビデオレコーダ 4 によって受信され、記録される。本発明によれば、データは、バス B 内に常に暗号形式で流れ、ネットワークのローカル秘密鍵  $K_{P R I . L o c}$  を收容する装置だけが制御語 C W を復号化し、データ D E を復号化し得る。したがって、これは、図 1 の家庭用ネットワークで作成された全てのコピーが他のローカルネットワークへブロードキャストされることを阻止される。

【 0 0 4 0 】

図1の例の場合に、回路12乃至15は、スマートカード11と一体化してもよいが、他の変形例では、回路D E M U X及び回路M U Xはデコーダ10に収容し、残りの回路13及び回路14がスマートカードに一体化される。とくに、回路C A 1 3及び変換器回路14は、復号鍵及び暗号鍵を収容するので、これらの回路は、スマートカードのような安全な媒体に組み込まれる。

【 0 0 4 1 】

提示装置2は、スマートカード21を搭載したスマートカードリーダーを具備したデジタルテレビジョン受像機(D T V 1) 20を含む。受像機20は、バスBを介して、デコーダ10、若しくは、デジタルビデオレコーダ4から発生されたデータストリームF'を受信する。データストリームF'は、スマートカード21へ送信される。データストリームF'は、デマルチプレクサ回路(D M U X) 22で受信され、デマルチプレクサ回路(D M U X) 22は、スクランブルをかけられたビデオデータパケット及びオーディオデータパケットD Eを、スクランブル解除回路(D E S . ) 24へ送信し、変換された制御メッセージL E C Mを端末モジュール23へ送信する。端末モジュールは、ネットワークの公開鍵(K<sub>P U B . L o c</sub>)と秘密鍵(K<sub>P R I . L o c</sub>)のペアを収容する。制御メッセージL E C Mは、ネットワークのローカル公開鍵K<sub>P U B . L o c</sub>を用いて暗号化された制御語C Wを収容するので、端末モジュールは、ネットワークのローカル公開鍵K<sub>P U B . L o c</sub>を用いて、これらの制御語を復号化することができ、制御語C Wを平文で取得することができる。これらの制御語C Wは、スクランブル解除回路24へ送信され、スクランブル解除回路24は、データパケットD Eのスクランブルを外すためこれらの制御語C Wを使用し、平文のデータパケットD Cをテレビジョン受像機20へ出力する。

【 0 0 4 2 】

平文データD Cがスマートカード21と、テレビジョン受像機20のディスプレイ回路との間で最終的に伝送されることを確保するため、スマートカードと、受像機20のカードリーダーとの間のインタフェースIは、スマートカードの安全性を確保するため、たとえば、米国N R S S標準(ナショナル・リニューワブル・セキュリティ・スタンダード)に準拠して作成される。

## 【 0 0 4 3 】

第2の提示装置3は、スマートカード31が搭載されたスマートカードリーダーを具備したデジタルテレビジョン受像機(DTV2)30を含み、第1の提示装置2と全く同様に動作するので、これ以上の説明を加えない。

## 【 0 0 4 4 】

上述のローカルデジタルネットワークを用いることにより、コンテンツプロバイダから生じたデータストリームFは、データストリームFを受信するアクセス装置によって、ネットワークのローカル公開鍵 $K_{pub, loc}$ を用いてデータストリームF'へ変換される。このデータストリームF'は、ローカルネットワークに特有のフォーマットを有し、このデータは、ローカルネットワークのローカル秘密鍵を保持するこのローカルネットワークの提示装置以外の装置では復号化し得ない。

## 【 0 0 4 5 】

次に、図1のローカルデジタルネットワークが作成される態様、及び、ネットワークの全ての装置がネットワークの固有のローカル鍵のペアを共用することを保証するように、新しい装置のこのローカルネットワークへの接続が管理される態様を説明する。

## 【 0 0 4 6 】

本発明によるデジタルネットワークを作成するため、アクセス装置と提示装置を一体的に接続する必要がある。

## 【 0 0 4 7 】

図2では、最初に、ネットワークは、デジタルバスBを用いて、アクセス装置1と提示装置2を接続することにより作成される場合を考える。ネットワークを作成する処理の種々の手順は、二つの装置の間で行われるやり取りを示すような形で時間軸tに沿って表わされている。

## 【 0 0 4 8 】

この処理の第1のステップ100において、2台の装置が一つに接続されたとき、提示装置は、公開鍵 $K_{pub, 2}$ と秘密鍵 $K_{pri, 2}$ のペアを収容し、本発明によれば、バージン状態にある。

## 【 0 0 4 9 】

装置の状態は、好ましくは、提示装置の端末モジュール23（図1）に設けられた2ビットのレジスタである状態インジケータIEによって記憶される。慣例的に、装置がバージン状態であるとき、状態インジケータIEは00に一致し、装置が親状態であるとき、 $IE = 01$ であり、装置が無効状態であるとき、 $IE = 10$ であるとする。

## 【 0 0 5 0 】

状態インジケータIEは、耐タンパー性が保証されるように、スマートカード内の集積回路に収容される。

## 【 0 0 5 1 】

提示装置が製造元によって販売されたとき、本発明のタイプの既設のローカルネットワークに接続可能でなければならない。また、提示装置は、新しいネットワークを作成するようにアクセス装置へ接続可能でなければならない。そのため、本発明に従って製造された提示装置は、提示装置毎に固有であり、他の提示装置のものとは異なる公開鍵と秘密鍵のペアを必ず保持し、これにより、本発明に従って作成された各ローカルネットワークが、ユニークな鍵のペアを保持することを保証する。さらに、やり取りの機密性を保証するため、使用される全ての秘密鍵／公開鍵のペアは、当業者に公知の方法に応じて照明される。

## 【 0 0 5 2 】

アクセス装置は、暗号鍵／復号鍵を保持しない状態で製造、販売される。アクセス装置は、好ましくは、図1に関して説明したように、本発明による（スマートカードに収容された）変換器回路を含み、接続されるネットワークのローカル鍵を記憶することができる。

## 【 0 0 5 3 】

図2を参照するに、この処理のステップ101において、提示装置2は、バス2を介して、バスBに接続される資格のある全てのアクセス装置、本例では、アクセス装置1を宛先として公開鍵 $K_{pub2}$ を配布する。

## 【 0 0 5 4 】

ステップ102において、アクセス装置1は、公開鍵 $K_{pub2}$ を受信し、ネ



ットワークの新しいローカル公開鍵 ( $K_{PUB, Loc} = K_{PUB, 2}$ ) として記憶する。

【 0 0 5 5 】

ステップ103において、アクセス装置1は、バスBを介して、提示装置2を宛先として、状態変更信号を配布する。このステップは、最初にネットワークへ接続すべきこと、並びに、ネットワークの親になるべきことを提示装置2に報せることを目的とする。換言すると、この提示装置2が秘密鍵  $K_{PR, 2}$  をネットワークへ接続されるべき新しい提示装置へ送信することが許可された唯一の提示装置である旨を提示装置2へ報せる。

【 0 0 5 6 】

ステップ104において、提示装置2は、状態変更信号を受信し、親状態 ( $IE = 01$ ) へ移るように状態インジケータを変更する。

【 0 0 5 7 】

この処理の最後に、ネットワーク中の装置に公開された (提示装置2の初期公開鍵  $K_{PUB, 2}$  と等しい) 固有のローカル公開鍵  $K_{PUB, Loc}$  と、提示装置2だけが知っている固有のローカル秘密鍵  $K_{PR, Loc}$  を有する本発明によるローカルデジタルネットワークが得られる。ネットワークは、本は詰めによれば、新しい提示装置の接続を許可することによりネットワークを変更することができる親提示装置を含む。

【 0 0 5 8 】

次に、図3を参照して、本例の場合に提示装置3である新しい提示装置を、図2の処理に従って作成されたネットワークへ接続する処理を説明する。

【 0 0 5 9 】

この処理の最初のステップ200、200' 及び200'' において、提示装置3を、デジタルバスBを介して、既存のローカルネットワークへ接続する。提示装置3は、固有の公開鍵  $K_{PUB, 3}$  と秘密鍵  $K_{PR, 3}$  のペアを収容し、バージョン状態 ( $IE = 00$ ) である。アクセス装置1及び提示装置2は、図2の処理の最後の状態と同じ状態であり、アクセス装置1は、ネットワークのローカル公開鍵  $K_{PUB, Loc}$  を保持し、提示装置は、ネットワークの親状態 ( $IE = 01$ )

）であり、ネットワークのローカル鍵のペア  $K_{PUB, LOC}$  及び  $K_{PRI, L}$  を保持する。

【 0 0 6 0 】

第2のステップ201において、提示装置3は、バスBを介して、バスBへ接続する資格のある全てのアクセス装置、本例の場合には、アクセス装置1へ向けられた公開鍵  $K_{PUB}$  を配布する。このステップは、作成処理のステップ101（図2）と同じステップである。

【 0 0 6 1 】

ステップ202において、アクセス装置1は、公開鍵  $K_{PUB}$  を受信し、アクセス装置1が既に公開鍵を保持しているかどうかを照合する。

【 0 0 6 2 】

本例のように照合結果が肯定的である場合、次のステップ203において、アクセス装置1は、バスBを介して、新しい提示装置3へ向けてローカル公開鍵  $K_{PUB, LOC}$  を配布する。

【 0 0 6 3 】

ステップ204において、提示装置3は、ローカル公開鍵  $K_{PUB, LOC}$  を受信し、そのローカル公開鍵を好ましくは端末モジュールに記憶する。

【 0 0 6 4 】

ステップ205において、提示装置3は、バスBを介して、ネットワークの全ての提示装置へ、ネットワークの親装置が応答することを要求するメッセージの形式（Genitor?）で信号を配布する。

【 0 0 6 5 】

ステップ206において、ネットワークの親装置、本例の場合に、提示装置2は、このメッセージを受信し、提示装置2と提示装置3の間で信頼できる形で通信が確立された後、提示装置2は、無効状態（IE = 10）へ移るように状態を変更する。

【 0 0 6 6 】

ステップ207において、提示装置2は、ネットワークのローカル秘密鍵を、提示装置3によって復号化可能な暗号形式（E（ $K_{PRI, LOC}$ ））で配布す

る。特に、提示装置2と提示装置3の間におけるこのローカル秘密鍵の安全な伝送は、ローカル秘密鍵を暗号化するための提示装置3の初期公開鍵 $K_{PUB}$ を用いて行われ、提示装置3は、この秘密鍵 $K_{PRIV}$ を用いてこのメッセージを復号化することができる。鍵 $K_{PUB}$ は、たとえば、ステップ205の間に提示装置2へ送信される。

【0067】

ステップ208において、提示装置3は、このローカル秘密鍵を受信し、好ましくは、スマートカード31（図1）と一体化された端末モジュールへ記憶させる。

【0068】

ステップ209において、提示装置3は、ローカル秘密鍵の受信を承認する信号を、バスBを介して提示装置2へ配布する。

【0069】

ステップ210において、提示装置2は、この受信承認信号を受信し、これに応答して、状態変更信号を新しい提示装置3へ配布し、ステップ211において、提示装置3は、この信号を受信し、ネットワークの新しい親になるように状態を変更する（ $IE=01$ ）。

【0070】

提示装置2は、これ以降、無効状態になるので、ネットワークのローカル公開鍵を他の提示装置へ送信することが許可されなくなる。これにより、上述のネットワークと同じローカル鍵のペアを保有する別の不正なローカルネットワークを作成するため、この装置2をネットワークから取り除くことが阻止できるようになる。

【0071】

この処理の最後に、2台の提示装置2及び3と1台のアクセス装置1とが、ローカルネットワークに接続されている。これらは、ネットワークのローカル鍵のペア $K_{PUB, Loc}$ 及び $K_{PRIV, Loc}$ を共用する。ネットワークには、常に、ネットワークに最後に接続された提示装置、すなわち、固有の親装置が存在する。

【 0 0 7 2 】

本発明によるアクセス装置が鍵を備えることなく販売されるので、新しいアクセス装置のローカルネットワークへの接続は、非常に簡単である。特に、新しいアクセス装置がネットワークにプラグインされたとき、新しいアクセス装置が、バスBを介して、ネットワークの公開鍵を受信することを要求するメッセージを配布するよう構成することが可能である。このメッセージを受信する第1のネットワーク装置、或いは、親装置だけが、このメッセージに応答して、ネットワークの公開鍵を新しいアクセス装置へ配布するよう構成することが可能である。

【 図面の簡単な説明 】

【 図 1 】

本発明によるローカルデジタルネットワークの説明図である。

【 図 2 】

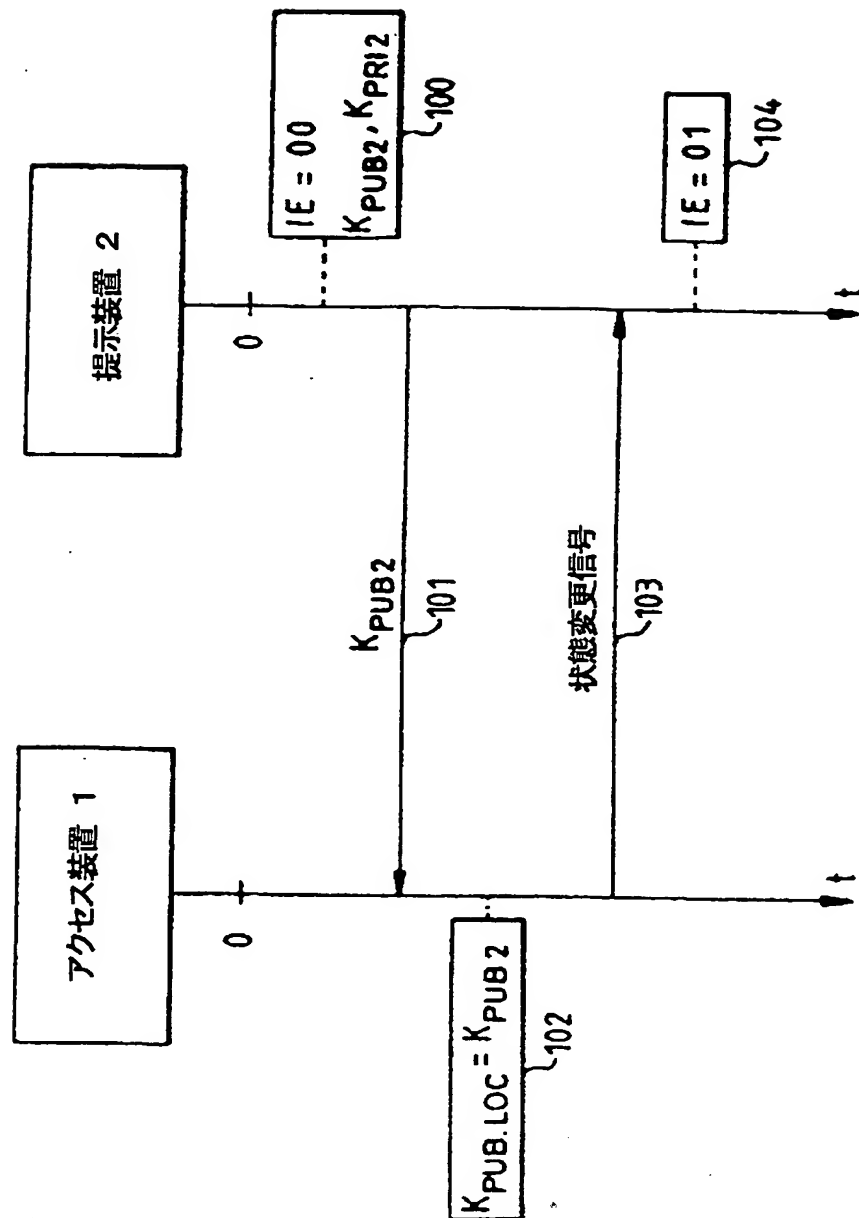
図1に示されたローカルデジタルネットワークのようなデジタルネットワークを作成する方法の説明図である。

【 図 3 】

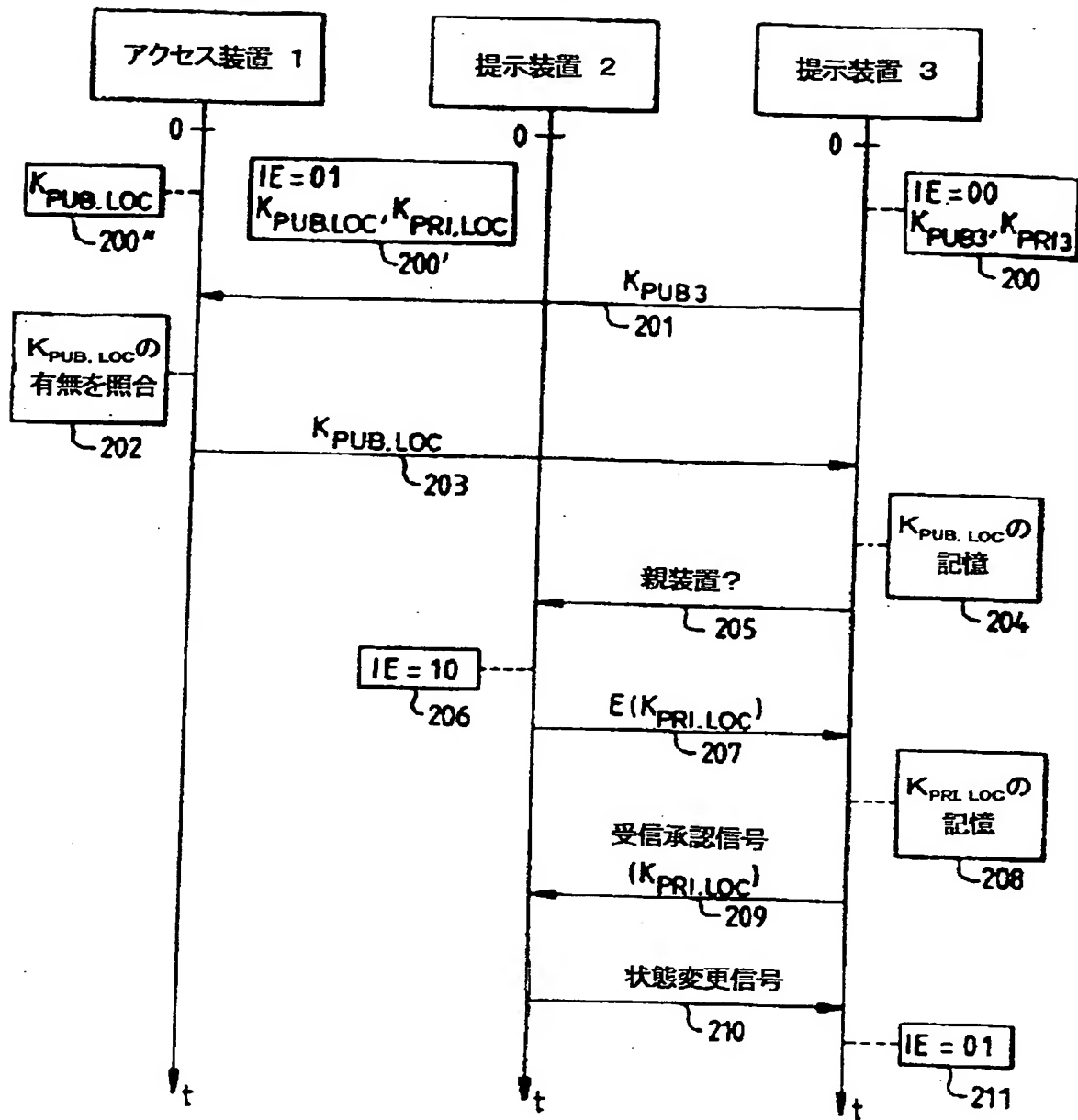
新しい提示装置を、たとえば、図2に示された方法に従って作成されたローカルデジタルネットワークへ接続する方法の説明図である。



【 図 2 】



【 図 3 】



## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

		Int. Application No. PCT/EP 00/02918
<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 H04L29/06 H04L12/28		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04L H04N		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 382 296 A (N.V. PHILIPS GLOEILAMPENFABRIEKEN) 16 August 1990 (1990-08-16)	1
A	column 2, line 2-37 column 3, line 12-29 column 4, line 40-44 column 4, line 55 -column 5, line 34 column 6, line 57 -column 7, line 5 column 8, line 56 -column 9, line 42	2-14
A	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 October 1995 (1995-10-25) page 2, line 22-41 page 3, line 31-34 page 3, line 47-50 page 7, line 34-57 page 9, line 46-57	1-14
<input type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (see specification) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "Z" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
11 July 2000		21/07/2000
Name and mailing address of the ISA European Patent Office, P.O. 5018 Patentlaan 2 NL - 2220 HW Rijswijk Tel. (+31-70) 340-2040, Tx. 31 661 epo nl, Fax: (+31-70) 340-3016		Authorized officer  Lázaro López, M.L.



## INTERNATIONAL SEARCH REPORT

information on patent family members

Inter. Appl. No.

PCT/EP 00/02918

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 382296 A	16-08-1990	NL 8900307 A	03-09-1990
		AU 620298 B	13-02-1992
		AU 4911190 A	16-08-1990
		CA 2009290 A	08-08-1990
		CN 1045317 A, B	12-09-1990
		DE 69011543 D	22-09-1994
		DE 69011543 T	02-03-1995
		JP 2250439 A	08-10-1990
		KR 155373 B	16-11-1998
		US 4980912 A	25-12-1990
		US 5144662 A	01-09-1992
EP 0679029 A	25-10-1995	US 5237610 A	17-08-1993
		EP 0683614 A	22-11-1995
		AT 144670 T	15-11-1996
		AT 181196 T	15-06-1999
		AT 180373 T	15-06-1999
		AU 650958 B	07-07-1994
		AU 1384092 A	01-10-1992
		BR 9201106 A	24-11-1992
		CN 1066950 A, B	09-12-1992
		DE 69214698 D	28-11-1996
		DE 69214698 T	06-03-1997
		DE 69229235 D	24-06-1999
		DE 69229235 T	23-09-1999
		DE 69229408 D	15-07-1999
		DE 69229408 T	11-11-1999
		EP 0506435 A	30-09-1992
		JP 5145923 A	11-06-1993
		SG 44801 A	19-12-1997

## フロントページの続き

(51) Int. Cl. <sup>7</sup>	識別記号	FI	キーワード(参考)
G 0 9 C 1/00	6 6 0	G 0 6 K 19/00	Q
		H 0 4 L 9/00	6 0 1 F

(81) 指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(72) 発明者 アンドル, ジャン・ピエール  
 フランス国, 35000 レヌヌ, リュ・ド・  
 ロンジェニル 20  
 (72) 発明者 フュロン, テディ  
 フランス国, 35000 レヌヌ, リュ・ド・  
 ラ・サンテ 13

Fターム(参考) 5B017 AA06 BA07 CA16  
 5B035 AA13 BB09 BC03 CA11  
 5B085 AE29 BC00  
 5J104 AA01 AA13 JA21 NA02 PA07

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**